REMARKS

Support for the subject matter in independent claim 28 is found in paragraphs [0051]-[0054] of the published application (concerning the lists of non-filtered domains and filtered domains, and how those lists are processed against extracted domain identifiers). Support for the subject matter in dependent claims 29-30 is found in paragraphs [0055—[0056] (relating to the use of multiple "client profiles"). No new matter has been included.

Claims 1-3, 4-12, 14-21 and 23-27 are rejected under 35 USC §103(a) as being unpatentable over Nilsson et al, WO 99/64967, in view of Dragulev et al, U.S. Publication No. 2001/0037407. Dragulev is newly-cited. With respect, this new rejection fares no better than the prior one and is <u>traversed</u>, as the Examiner continues to mis-apply Nilsson to the claimed subject matter. For the reasons set forth below, reconsideration and favorable action are requested.

"[A]n applicant can overcome a [Section 103] rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case, …" *See*, *In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). In considering this question, it is appropriate to consider whether the Examiner has met his or her burden to show that the claimed subject matter is disclosed "clearly and unequivocally" in a cited reference. *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972). This issue is evaluated from the viewpoint of a person of ordinary skill in the art, who is a person of ordinary creativity, not an automaton. *KSR Int'l Co. v. Teleflex, Inc.*, 55o U.S. 398, 421, 127 S.Ct. 1727 (2007).

Whether or not particular subject matter "as a whole" would have been obvious to one of ordinary skill in the art at the time an invention was made depends on underlying factual inquiries including: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; and (3) the differences between the prior art and the claimed invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In rejecting claims under 35 U.S.C. § 103(a), it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See*, *In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988).

Independent claims 1, 10 and 19

By way of brief background, the subject matter of this application relates generally to a privacy proxy server or privacy service. If a user of such a system or service is very mobile and

uses many different client devices, there may be occasions or environments in which the user would like to receive some or all "cookies" (typically, HTTP files produced by web servers) that include tracking information at a client device while filtering out some or all cookies in a different environment or on a different occasion, even though the user may or may not continue

5   to employ a privacy proxy or privacy service in these different environments or upon these different occasions. For example, if a user only accesses a certain web site from the user's personal laptop and never from an office desktop, then the user may want to allow cookies through the privacy proxy server to the laptop; the laptop would tend to have the latest cookies stored in its cookie cache, which might be important for certain sites that are highly customized

10   or individualized. In this example, the user's laptop would have recent cookies if the user decided to use the laptop without accessing the Web through the privacy proxy server.

With the subject matter described herein, the user is able to create different client profiles based on the user's needs, thereby giving the user a finer granularity of control over the cookie filtering functionality of a privacy proxy server or a privacy service. In particular, with the

15   described subject matter, the user can *customize* the operation of the privacy proxy server or the privacy service on the basis of *user-configured* information. The privacy proxy then filters cookies that are returned by the server *in accordance with user-configurable parameters*.

Nilsson illustrates a proxy server 66 located between a mobile device user terminal 52 having a browser 54, and a server 70. In Nilsson, the goal is to intercept and store a cookie

20   generated by the server 70 so that the user terminal 52 <u>does</u> <u>not</u> <u>need</u> to store the cookie. In operation, the client makes a request to the server, which then provides a response together with the cookie. This is a conventional server operation. Rather than passing the cookie back to the user terminal, the cookie is stored in the proxy together with information identifying the requested URL and the user terminal. In that manner, "the next time" the user terminal 52

25   accesses the server 70, the proxy server 66 matches the requested URL and the identification information and in this manner finds the previously-stored cookie. The cookie is then provided to the server 70 with the request. Thus, the cookie is stored in the proxy server 66 and need not be transmitted over a wireless interface.

Dragulev describes a system and method for managing user-specific data communicated over a network independent of devices that are used to communicate. A profile client (a software application) is associated with a user device. The profile client is operable to retrieve (from a profile server) user-specific data associated with a user currently logged into the user device.

5   The profile client stores the retrieved user-specific data on the user device so that such data can be used (as user-specific data for the user) when communicating to network nodes during the time that the user is logged into the user device. The profile client can insert the user-specified data in a communication from the user device to one of the network nodes; also, the profile client can intercept data communicated from a network node to the user device and extract user-

10   specific data that it can then store in the profile server. In this manner, the user-specific data is maintained over multiple user sessions, independent of devices that the user uses to communicate with the network nodes. As described in [0098], which is the paragraph relied upon by the Examiner, the profile client can provide a configuration page to enable the user to create a "deny" list, a "list of addresses or names of senders whose cookies the user would like to filter out."

15   In the "new" rejection, the Examiner contends that Nilsson discloses all of the elements of independent claims 1, 10 and 19 except the limitation directed to a "set of parameters" wherein the "parameters comprise domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers." (See, Office action at pages 3-4)[1] This element, however, is said to be met by the secondary reference, Dragulev. That

20   teaching aside, and with all due respect, the Examiner has mis-applied Nilsson, which reference does not teach all of the other elements of each independent claim.

In particular, the Examiner argues (at page 4, last paragraph) that Nilsson performs the step of "extracting from the response message a domain identifier associated with the server." This is incorrect; what actually happens at the Nilsson proxy server 66 is the exact _opposite_ step,

25   because at this point in the Nilsson processing the proxy 66 operates _on the request message_ from the end user terminal and not _the response message_ from the server 70. This distinction is clear

---

[1] These contentions are not new, however. They are the same arguments presented in the Office action mailed August 5, 2008.

from the very portion of the Nilsson text relied upon by the Examiner, namely, the text at page 3, lines 9-11 (emphasis supplied):

"Thus, when a remote HTTP server or the like is contacted by a user terminal and the remote server transmits a cookie to the user terminal, the cookie is intercepted and stored in the proxy server. Information regarding the remote server, e.g., its URL[,] and an identification identifying the user terminal or the user is stored together with the cookie. The next time the user terminal or the user accesses the same HTTP server the proxy server matches the requested URL and the identification information and in this manner finds the stored cookie. The cookie is then added to the request message so that the remote server is accessed with a copy of the cookie as desired."

At this stage in the Nilsson operation, the "domain identifier" – if any – is the URL in the client request message, as opposed to the domain identifier in any server response message. Thus, the portion of the text relied upon by the Examiner does not meet the claim limitation itself.

Moreover, the final step of claim 1 requires "processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier." As noted in the previous paragraph, the "extracted domain identifier" referenced at this part of the claim refers to the prior "extracting" step where the "domain identifier" is extracted from the server response message; as noted above, the URL obtained by the proxy at this point in the Nilsson operation is an identifier taken from the end user request message itself. In other words, in the Nilsson operation (and after the cookie is stored at the proxy), when the end user terminal issues a next request to the server, the proxy determines whether there is a stored cookie and, if so, the proxy merely attaches the cookie to the request before passing the request to the server. The cookie itself is not processed "in accordance with [any] retrieved set of parameters and the extracted domain identifier." Stated another way, in Nilsson at most what happens is that the cookie is re-attached to the end user terminal request – i.e., the client request, not the server response - before that request is passed on to the server.

Nilsson cannot disclose the "processing the cookie" step as claimed because it never extracts a domain identifier from any server response message; at most, Nilsson's proxy extracts

some information from the <u>client request message</u> during a subsequent request (the "second time around"), but that it not what is being claimed here. In considering grounds of rejection, "every limitation in the claim must be given effect rather than considering one in isolation from the others." See, <u>*In re Geerdes*</u>, 491 F. 2d 1260, 1262-63 (CCPA 1974); <u>*In re Steele*</u>, 305 F. 2d 859,

5   862 (CCPA 1962).   Further, every limitation in a claim is material to patentability. (*See*, 35 U.S.C. §103(a) concerning the subject matter "as a whole").

       Further, Nilsson does not disclose proxy server <u>filtering</u> of a cookie that is being <u>returned</u> from a server to a client, let alone per-domain cookie filtering. As is evident from the above description, Nilsson has nothing to do with cookie blocking; rather, the entire point of that

10   scheme is to store cookies at the proxy so that they <u>do not have to be returned to the requested end user terminals</u>. Stated another way, in Nilsson there is no cookie blocking function because the whole purpose of the proxy is to store the server-generated cookies. There is no function in Nilsson that selectively "block[s] transmission of cookies" (and then, conversely, allows such cookies to pass back through the proxy).   In particular, an end user of the terminal 52 cannot

15   configure the proxy 66 in any way to allow, let alone to allow some cookies to pass through while others are merely stored.

       As can be seen, Nilsson simply teaches cookie storage in the proxy to make it unnecessary to pass the cookie back to the requesting end user terminal, and then later re-using the cookie to obtain access to a resource on the server. This is not the subject matter of the

20   claims here. Rather, the claims here <u>assume</u> that the client has obtained access to the server and that the server has issued the cookie. Unlike the teachings in Nilsson, in pertinent part the claims concern whether that cookie <u>will be returned to the client</u>. As noted above, no cookies are ever returned to the requesting end user terminals 52 in the Nilsson scheme. This cookie processing concept is not disclosed or suggested by Nilsson, which does not address the question of how a

25   cookie being returned <u>from a server to the client</u> should be processed, let alone filtered according to <u>user-configurable</u> options. In particular, Nilsson does not describe providing a technique for enabling a user to configure at the proxy server per-domain (and, optionally, per-client profile) filtering of cookies that are returned from servers. Rather, Nilsson deals with an unrelated issue, *viz*., how to store and re-use a cookie so that the requesting end user terminal does not need to

store it directly. Stated another way, in Nilsson there is no cookie processing function because the whole purpose of the proxy is to store the server-generated cookies so that they can be re-used. In other words, there is no function in Nilsson that "process[es] the cookie." In particular, an end user of the terminal 52 cannot configure the proxy 66 in any way, let alone to

5   allow some cookies to pass through while others are merely stored.

Dragulev does not make up for these deficiencies. The reference is cited solely for its teaching of configuring "a list of addresses or names of senders whose cookies the user would like to filter out." Of course, by describing that a user can configure Dragulev to filter out cookies, this necessarily implies that cookies that are not filtered out are passed back to the client

10   browser. More importantly, this teaching notwithstanding, the independent claims are more directed in that they recite a specific set of operations that take place after the proxy receives "a response message from the server [and intended] for the client." In particular, it is at this point in the operation that the further "detecting," "extracting," "retrieving" and "processing" steps are carried out. (This is clear from the sequencing of the steps).

15   In particular, the combination of the cited art still fails to disclose at least the following steps of claims 1, 10 and 19:

"detecting at the proxy server a cookie associated with [a] response message;

extracting from the response message a domain identifier associated with the server;

retrieving [a] set of parameters; and

20   processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier."

One skilled in the art would not combine Nilsson and Dragulev as the Examiner has done here. In particular, in discussing the question of obviousness of a patent that claims a combination of known elements, *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 127 S.Ct. 1727

25   (2007), explains "when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." Id. at 1740 (citing United States v. Adams, 383 U.S. 39, 51-51 (1966). Additionally, "[a] reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction

divergent from the path that was taken by the applicant." _In re Kahn_, 441 F.3d 977, 990 (Fed. Cir. 2006) (quoting _In re Gurley_, 27 F.3d 551, 553 (Fed. Cir. 1994)). To "teach away," a reference typically should warn a person of ordinary skill in the art not to apply a certain structure or technique. _Para-Ordnance Mfg., Inc. v. SGS Importers Int'l, Inc._, 73 F3d 1085, 1090 (Fed.

5 Cir. 1995). See also, _In re Gordon_, 733 F. 2d 900 (Fed.Cir. 1984) (a proposed combination is improper if it renders a reference inoperable for its intended purpose).

Here, Dragulev enables a user to block certain cookies and to pass others, but one of ordinary skill in the art would never modify Nilsson to "process[ ] the cookie" (such as alleged to be suggested by Dragulev). In particular, and as noted above, one of ordinary skill in the art

10 would never modify Nilsson to pass the cookie back to the client (or not, as Dragulev would allow), as the entire Nilsson system is designed to avoid precisely that function. The reference specifically teaches "by storing cookie information in a proxy server, the cookies do not need to be stored in the user terminal, which in many cases have a small memory and which therefore is not suited for storing cookies." (See, page 9). Further, "when the user terminal is a mobile

15 terminal the cookie is not transmitted over an air-interface [back to the client], thereby reducing the amount of transmitted over the air interface significantly." (See, page 3) It would defeat the purpose of the Nilsson scheme to combine it with Dragulev (as the Examiner has done) so that end users could configure the combined system to pass cookies back to the client.

Thus, independent claims 1 (method), 10 (apparatus) and 19 (computer program product)

20 describe patentable subject matter.

Dependent claims 7-9, 16-18 and 25-27 are patentable for the reasons advanced with respect to the parent claims.

Dependent claims 2, 11 and 20 describe the cookie processing steps more specifically and, in particular, the steps of blocking the cookie from transmission, caching the cookie at the

25 proxy, and sending a modified response message to the client. This is the scenario such as described in steps 614, 618 and 620 of FIG. 6A, where the user has selected an option not to allow the cookie through the privacy service proxy server. As noted above, Nilsson has no concept of selectively blocking some cookies while allowing others to pass back through to the client, and one of ordinary skill would not modify this reference to do so. While Dragulev does

allow for cookie filtering, the combination still lacks the "processing the cookie … against the extracted domain identifier" requirement.

Dependent claims 3, 12 and 21 likewise describe the cookie processing steps but in this case describe the operation where the cookie (of a recognized domain) is <u>passed back</u> to the client. This is the scenario such as described in step 614 and 616 of FIG. 6A, where the user has selected an option to allow the cookie through the privacy service, in which case the privacy service sends the response to the client without removing or detaching the cookie from the response.

As described above, Nilsson teaches away from this requirement, *as cookies are retained at and by the proxy.* One of ordinary skill in the art would never modify Nilsson to pass the cookie back to the client, as the entire Nilsson system is designed to avoid precisely that function. In particular, the reference teaches away from the explicit claim requirement of "sending the response message along with <u>its associated cookie</u> to the client."

Moreover, these claims also include a conditional clause, namely, that the sending the response message function takes place "<u>in response to</u> a determination that the set of parameters contains the extracted domain identifier." As noted above, neither Nilsson nor Dragulev disclose or suggest making a determination that compares the "set of [user-configured] parameters" with the "domain identifier" extracted from the server "response message." Thus, the specific "in response to" operation cannot be (and is not) found in the Nilsson/Dragulev combination.

For all these reasons, claims 3, 12 and 21 are separately patentable over the combination.

Dependent claims 5, 14 and 23 are separately patentable as they describe the further step of determining if the set of parameters contains an indication that the user has enabled cookie processing by the proxy server. In one embodiment, this refers to determining whether a "source domain filter enable flag" (218) is set. This functionality is also absent from the Nilsson/Dragulev combination.

Dependent claims 6, 15 and 24 are separately patentable as they describe the further steps of managing "<u>multiple</u> sets of parameters <u>for the user</u>." This is a client profile option.

As noted above, the "set of parameters" referenced in the claim are parameters that "are configured <u>by the user at the client</u>."

The "set of parameters" referenced in the claim are parameters that "are configured by the user" and this set of dependent claims further requires "multiple" such "sets of parameters." Nilsson does not disclose or suggest multiple client profiles, and Dragulev's approach is to use a single client profile across multiple client devices.

5   Neither Nilsson nor Dragulev disclose or suggest "multiple" user-configurable "sets of parameters" that comprise "domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers."

With respect to these limitations, there is "insufficient evidence of *prima facie* obviousness." *See*, *In re Kahn*, 441 F.3d at 985-86.

10   For the reasons stated above, the obviousness rejections are in error and should be withdrawn.

New claims 28-30

As noted above, the new claims 28-30 describe a further aspect of this disclosure, namely that the user configurable "set of parameters" comprise a "list of non-filtered domains" and a

15   "list of filtered domains." The "extracted domain identifier" is processed against these lists in the manner described at paragraphs [0051]-[0054] of the published application. Thus, if the extracted domain identifier is on the non-filtered domain list, the response message (from the server) is simply passed to the client; if, however, the extracted domain identifier is not on the non-filtered domain list but is on the filtered domain list, the user has expressed a preference to

20   block the cookie and cache it in the proxy server. If, however, the extracted domain identifier is on neither the non-filtered domain list nor the filtered domain list, the user has not yet expressed a preference with respect to that domain (and the associated cookie); thus, the proxy server prompts the user to enter and parameter, which is then added to the set of parameters. This processing (against non-filtered and filtered domain lists) is not disclosed or suggested by either

25   Nilsson or Dragulev.

Dependent claims 29-30 describe the further feature of extending the per-domain configuration to multiple client profiles. As described in paragraph [0055] of the published application, this is a "combination" of source domain filtering and client profile filtering, which combination is once again absent from the cited references.

Respectfully submitted,

/David H. Judson/

By: _____

David H. Judson, Reg. No. 30,467

March 6, 2010